Software
Engineering
Center
Information-technology Promotion Agency, Japan

# ＳＥＣ統合系プロジェクトの取組み紹介
## ～統合システムの安全性・信頼性の確保に向けて～

2011年６月１７日


（独）情報処理推進機構
ソフトウェア・エンジニアリング・センター
統合系プロジェクトリーダー
立石 譲二

# SECの概要

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

## 目 的

エンタプライズ系ソフトウェアと組込み系ソフトウェアの開発力強化に取り組むとともに、その成果を実践・検証するためのエンピリカル・ソフトウェアエンジニアリングを採用し、産学官の枠組みを越えて展開。こうした活動から日本のソフトウェアの競争力向上を実現し、技術開発の推進・国際標準の獲得・中心となる人材の育成を図る。

## 組 織 情 報

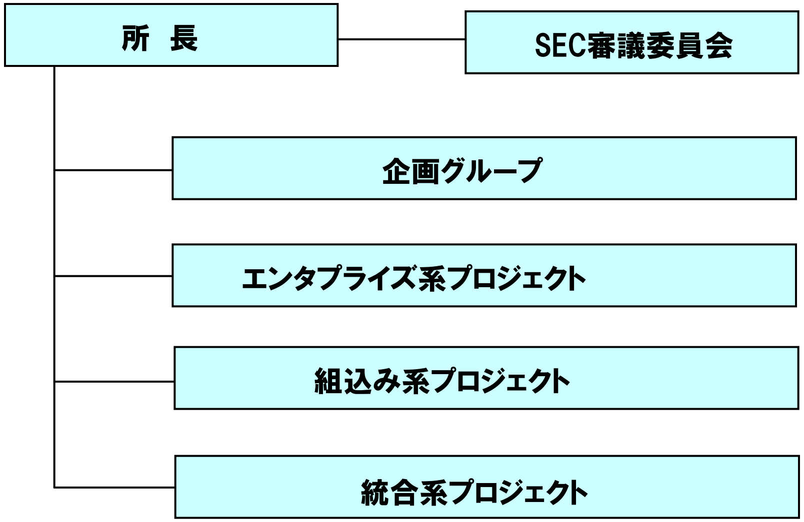
（１）名称： ソフトウェア・エンジニアリング・センター
(Software Engineering Center)

（２）設立： 2004年10月1日

（３）所長： 松田 晃一

（４）所員数（2011年4月1日現在）
： 45名

組織図（2011年4月1日現在）





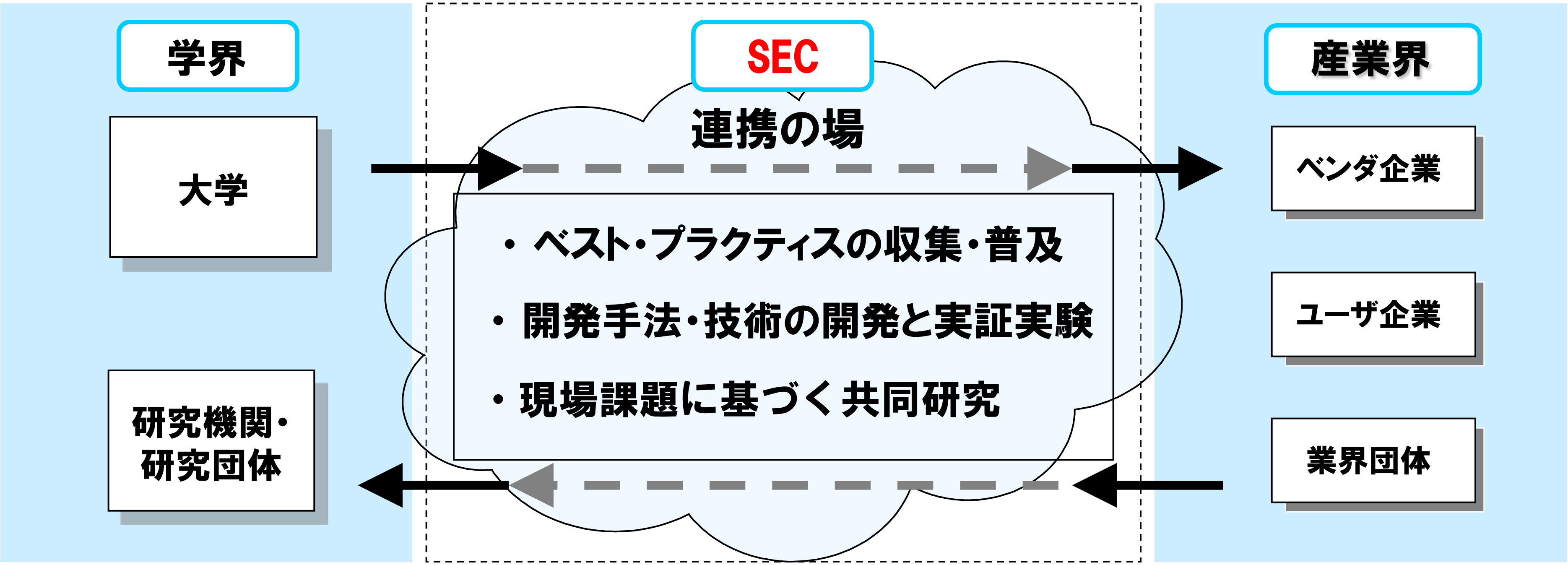
Copyright © 2011 IPA, All Rights Reserved

# ソフトウェア・エンジニアリング・センター

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

■ ソフトウェア開発の信頼性向上

■産学官の連携の場





Copyright © 2011 IPA, All Rights Reserved

# ① 第1期活動を通じた国内関係機関との連携

SEC
Software Engineering for Mo･No･Zu･Ku･Ri

# SEC成果のマップ

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

：ツール　：ダウンロード可　：標準化

| プロセス・アクティビティ（共通フレーム2007） | SEC成果 | 外部との連携（国際機関も含む） |
|---|---|---|
| 企画<br>システム要件定義<br>ソフトウェア要件定義<br>システム方式設計<br>ソフトウェア方式設計<br>ソフトウェア詳細設計<br>ソフトウェアコード作成及びテスト<br>システム結合<br>ソフトウェア結合<br>システム適格性確認テスト<br>ソフトウェア適格性確認テスト | 超上流<br>非機能要求<br>合意形成ガイドライン<br>コーディングガイド(ESCR),(ESCR C++版)<br>見積り<br>見える化（上流）<br>見える化（中流）<br>見える化（下流）<br>定量データ収集・分析（ソフトウェア開発データ白書2010-2011）<br>プロセス標準（共通フレーム2007）<br>プロセス改善<br>高信頼化ソフトウェアのための開発手法ガイドブック<br>組込み系開発プロセスガイド(ESPR)<br>組込み系開発プロマネガイド(ESMR)<br>続・定量的品質予測のススメ<br>信頼性ガイド<br>組込みスキル標準(ETSS) | 形式手法適用実証実験（国内DSF）<br>見積手法超上流企画（独IESE）<br>プロセス改善（米国SEI）<br>ソフトウェア品質保証（米国NIST）<br>モデルベース開発技法（仏LIST） |

Copyright © 2011 IPA, All Rights Reserved

## ■ ソフトウェア開発データ白書2010-11

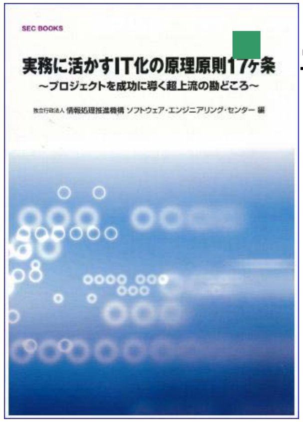
- 2010年11月発行
- 24社，2584件のデータ（累計）
- 見積りの参考になる規模測定要素と工数の関係を追加
- 生産性に関して業種別に分解し、発生不具合と相互の関連について分析

## ■ 共通フレーム2007　第2版

- 2009年10月発行
- 共通フレーム2007の改訂版
- 主な改訂内容
  - ・企画プロセス及び要件定義プロセスの整備
  - ・プロセス同士の参照関係　の見直し
  - ・第3部の作業項目及びガイダンスの強化
  - ・見積り、契約関係の情報付加　他

## ■ 続・定量的品質予測のススメ

- 2011年3月発行
- 目的は、IT業界の品質管理の全体的な底上げを図る事
- 品質予測の必要性や考え方、システム開発の各工程での品質予測のアプローチを、企業での実践ノウハウ、事例を基に体系的に整理
- ソフトウェア測定プロセスの国際規格、ソフトウェア信頼度成長モデルについて紹介




## ■ 実務に活かすIT化の原理原則17ヶ条

- 2010年10月発行
- ソフトウェア開発プロジェクトの成否は、システム要求事項をいかにして漏れなく・正確に定義するかにかかっており、2005年に、発注者と受注者が守るべき基本的な考え方と行動規範をまとめた原理原則17ヶ条を含め、「経営者が参画する要求品質の確保～超上流から攻めるIT化の勘どころ～」としてまとめ発行



Copyright © 2011 IPA, All Rights Reserved

# 事例１　：　ソフトウェア開発データの収集・分析

ソフトウェア開発プロジェクトのデータを企業から収集し，分析を加えた上で取りまとめ公開

- 世の中の傾向を把握し，施策に反映
- 自プロジェクトのデータを重ね，立ち位置を知り，開発管理にフィードバック

**収集情報**
約400項目

プロジェクト情報

規　模　　工　数　　工　期

生産性　　信頼性

出版：データ白書2009

出版：プロジェクトの定量的品質管理のススメ

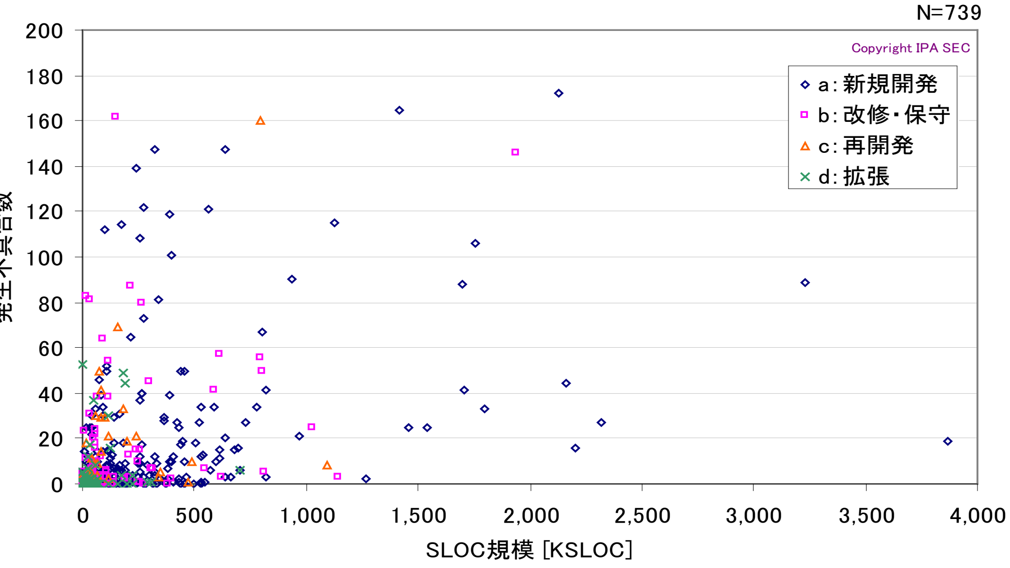
ツール提供：プロジェクト自己診断

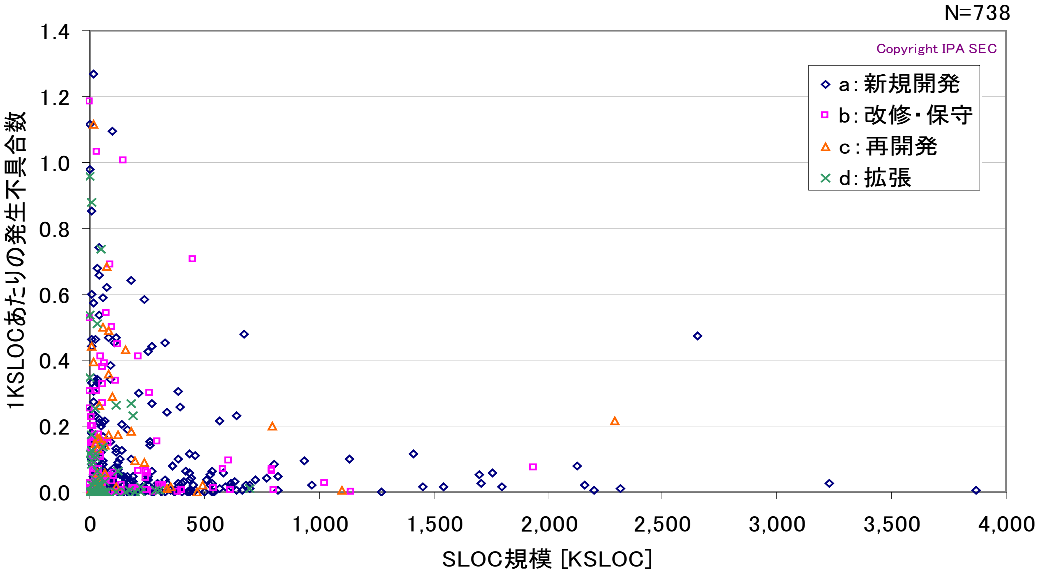
ツール提供：プロジェクト診断

# 定量データ分析の一例

## 規模と稼動後不具合の関係についての傾向の把握

| SLOC(プログラム規模)と発生不具合数 | SLOCと発生不具合密度 |
|---|---|




[件]

| 開発プロジェクトの種別 | N | 最小 | P25 | 中央 | P75 | 最大 | 平均 | 標準偏差 |
|---|---|---|---|---|---|---|---|---|
| 全体 | 739 | 0 | 0.0 | 1.0 | 7.0 | 1,262 | 15.4 | 70.0 |
| a：新規開発 | 400 | 0 | 0.0 | 2.0 | 9.3 | 1,262 | 20.1 | 88.4 |
| b：改修・保守 | 206 | 0 | 0.0 | 0.0 | 3.0 | 320 | 9.1 | 30.4 |
| c：再開発 | 46 | 0 | 1.0 | 4.5 | 18.8 | 500 | 24.7 | 76.4 |
| d：拡張 | 87 | 0 | 0.0 | 0.0 | 1.0 | 53 | 3.7 | 10.3 |

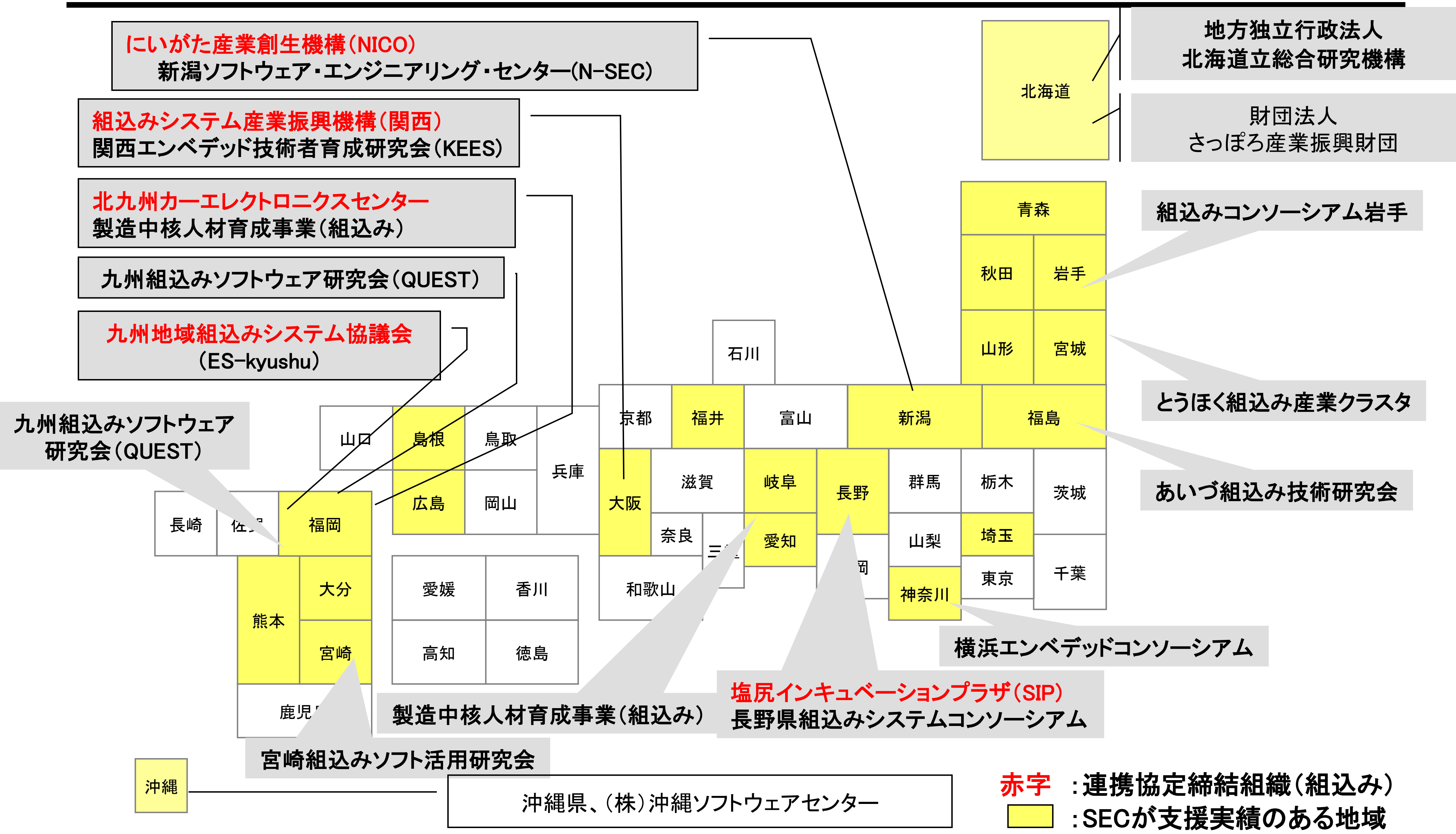
[件／KSLOC]

| 開発プロジェクトの種別 | N | 最小 | P25 | 中央 | P75 | 最大 | 平均 | 標準偏差 |
|---|---|---|---|---|---|---|---|---|
| 全体 | 738 | 0.000 | 0.000 | 0.011 | 0.078 | 5.845 | 0.123 | 0.426 |
| a：新規開発 | 400 | 0.000 | 0.000 | 0.020 | 0.067 | 4.708 | 0.107 | 0.333 |
| b：改修・保守 | 205 | 0.000 | 0.000 | 0.000 | 0.066 | 5.845 | 0.156 | 0.628 |
| c：再開発 | 46 | 0.000 | 0.008 | 0.092 | 0.251 | 2.041 | 0.205 | 0.354 |
| d：拡張 | 87 | 0.000 | 0.000 | 0.000 | 0.033 | 0.957 | 0.073 | 0.182 |

全開発種別：SLOC,主開発言語混在

# 地域における組込み関連のSEC支援状況(抜粋)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri



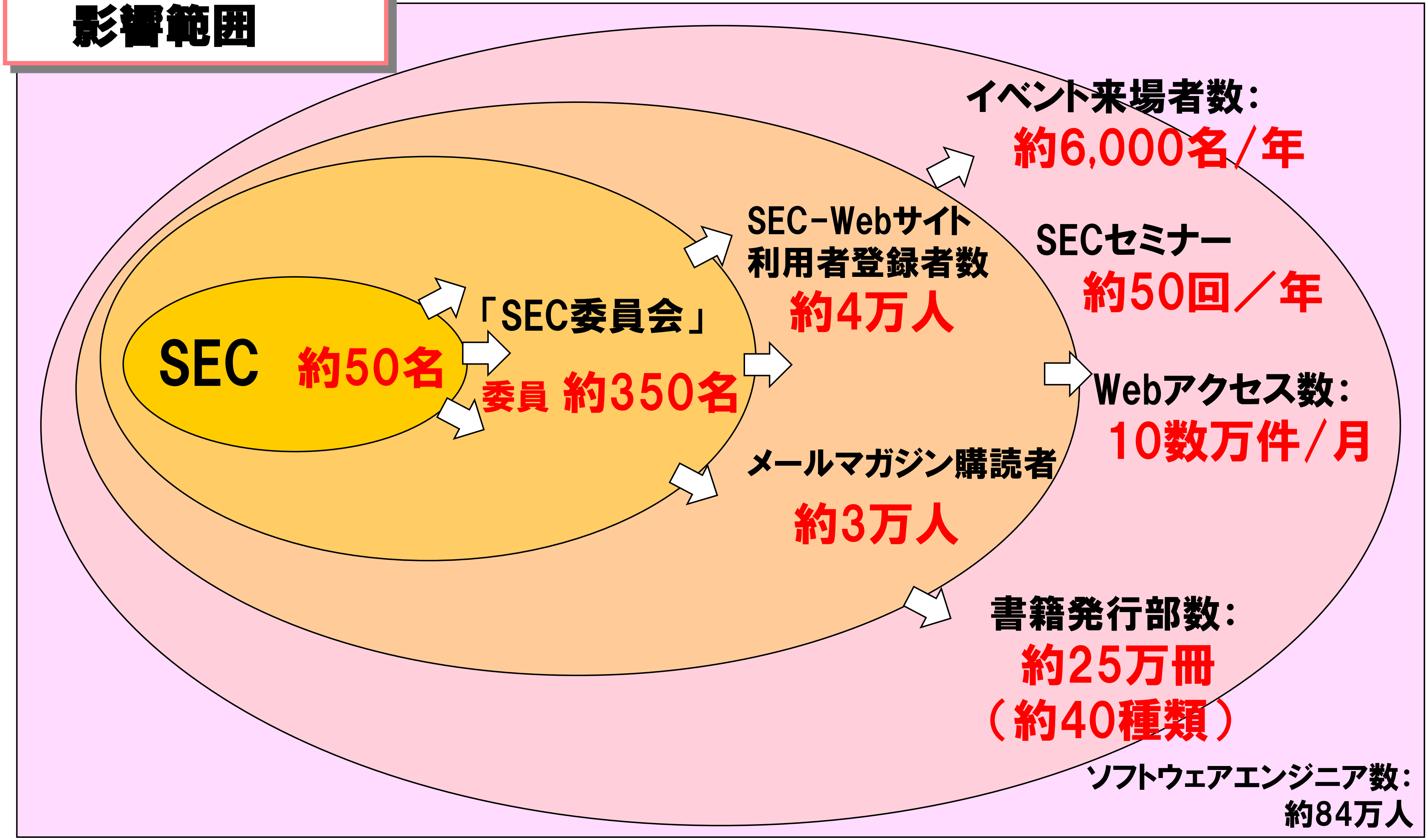


Copyright © 2011 IPA, All Rights Reserved

# SEC活動の広がり

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

## 影響範囲





Copyright © 2011 IPA, All Rights Reserved

# ５．第2期中期計画 （`08～`12年度） の基本方針

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

「ソフトウェア開発力の強化 」（第1期2004～2007年）から
「情報システムの信頼性向上」（第2期2008～2012年）へ

1. システムの開発段階だけでなくシステムの企画段階から保守段階までの全ライフサイクルに検討対象を広げる

2. ベンダ企業だけでなくユーザ企業にも役立つ成果を目標に検討範囲を広げる

3. 一般国民の安心・安全の確保に貢献することを目指す

# 2011年度計画

## 2-1　ITシステムの信頼性確保

（2-1-1）ソフトウェア品質監査の枠組み作り

（2-1-2）高信頼ソフトウェア開発・管理技術

- （ｉ）上流における信頼設計過程の強化
- （ii）組込みの高信頼化設計、テスト技術
- （iii）要求・仕様の高品質化
- （iv）開発プロジェクトデータの収集・分析
- （ｖ）障害情報の収集・分析
- （vi）高信頼システムの構築・運用対策の見える化
- （vii）プロセス改善

（2-1-3）信頼性向上対策の普及・推進

（2-1-4）信頼性対策の効果の調査・評価


Copyright © 2011 IPA, All Rights Reserved

# 統合系プロジェクトにおける取組み紹介

- ソフトウェア品質に係る第三者検証制度の構築に向けた検討
- ソフトウェア・システムの高信頼化技法に関する実証の推進

# 2．統合システムの信頼性について
## 国民生活に直結する情報システムの信頼性（国内編）

SEC
Software Engineering for Mo･No･Zu･Ku･Ri

| 日付 | 不具合事例 | 不具合原因 |
|---|---|---|
| 2007年3月2日 | **au3機種64万台に不具合**<br>使い方によってフル充電できず、電池劣化が進行する可能性 | 充電機能の**ソフトウェア不具合** |
| 2007年5月27日 | **全日空国内線予約システム故障**<br>130便が欠航、影響は4万人以上、キャンセルなどによる損失4.5億円 | 空港端末とホストコンピュータをつなぐ**ルータ管理プログラムの設定ミス**によるメモリー故障が発端で全システムに波及 |
| 2007年10月12日<br>2007年10月18日 | **自動改札機起動せず**<br>**PASMO-Suica窓口処理機で異常発生** | ともに、中央コンピュータからのデータをICカードに書き込む**プログラムにミス** |
| 2008年7月22日 | **東京証券取引所のシステム障害**<br>東証株価指数やTOPIXオプション、国債先物取引などの派生商品の売買不可 | **単純なプログラムミス**（4けたの数字を入力しなければならないところを誤って「4」と入力） |
| 2009年8月28日 | **北米トヨタ車レクサスの暴走による死亡事故**<br>レクサスが高速道路で暴走し、ブレーキが効かず運転手含む4名が死亡。フロアマットの改修と230万台のリコールを実施。 | フロアマットとは別に、スロットル電子制御システムの欠陥の疑いが議会から追求されNASAでの検証が行われたが、プログラム上の不具合は発見されず。**開発者側のシステム品質の説明力の限界を印象づけた出来事** |
| 2011年3月18日 | **みずほ銀行**<br>3月15日から特定口座の振り込み処理で発生したシステムトラブルを発端に全てのATMの利用及び振り込み処理が停止し、給与振り込み等最大116万件の決済処理が滞った。 | 被災地義援金を募集した都内一部支店の複数口座について、システム上の上限を超える取引が集中した結果、約一週間に及ぶ大規模なシステム障害に発展した。**義援金受付口座に対する行員の上限設定ミス** |

# 国民生活に直結する情報システムの信頼性（全世界編）

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 至る所に障害の原因は潜んでいることが推測される。
- 重篤度の高い障害は、航空管制・鉄道運航管理系のシステム。

注）番号は「重要インフラ」別の整理番号、「重大」事例については経済的損失額、障害復旧時間各々の大きい順に羅列、（ ）内は被害

← 原　因　（推定含む）→

| 重篤度 | 元々の仕様・設計・構築に不具合（仕様要求不足・考慮漏れ含む） | 運用・保守時に発生（アップグレード・リプレース時） | 人為的なミスにより発生（管理ミス、運用ミス等） |
|---|---|---|---|
| 破局的（死傷者発生・その潜在性大） | 17. Boeingグアム墜落事故（死者228名）<br>22. 英Paddington列車衝突事故（死者31名）<br>32. 英Buncefield油槽所火災（警報不良） | 19. 米航空管制システム障害（管制官200名）<br>24. 独鉄道レール切替シス不具合（3日間）<br>23. 米道路交通信号機シス不具合（復旧半日） | 24. 米NY地下鉄衝突事故（仕様見直し不足） |
| 重　大（経済的損失大、広範囲・長期障害） | 18. 英航空管制SWバグ（開発費6.2億ポンド）<br>10. NASDAQシステム誤作動（復旧24時間）<br>7. 米長距離電話通信網ダウン（復旧9時間）<br>8. 英LSE株式売買システムダウン（復旧7時間）<br>25. 欧州停電（復旧最大4時間、最大6000万人）<br>30. 米社会保険金支払不足（約70万人）<br>31. 加医療情報シス不具合（約600人、復旧5日）<br>1. Verizon社料金過剰請求（復旧4日）<br>3. スウェーデン電話不通（復旧最大8時間） | 15. 北米銀行口座残高増加（7.6億ドル誤認）<br>16. 米NYSE取引停止（復旧75分）<br>14. 北投資家口座残高不足（復旧24時間）<br>11. 北米銀取引シス不具合（1億ドル、復旧2週間）<br>4. 加Northern電話交換シス不具合（復旧1カ月）<br>2. 米MCI-WorldCom NW障害（復旧8日間）<br>20. 米列車発券シス不具合（復旧最大3日間）<br>6. 米AOL NWダウン（復旧19時間）<br>5. 米Bell Atlantic電話シス不具合（復旧7時間）<br>9. 米地銀システムダウン（ATM停止等） | 26. 北東アメリカ大停電（人為的他複合原因）<br>21. 米シスコ高速鉄道停止（復旧最大70分） |
| その他（上記以外） | 12. 米銀ATM停止（復旧最大1日）<br>27. 米大統領選投票シス障害（復旧最大半日） | 28. 英納税システム不具合（約13万人）<br>29. 米財務省社会保険シス不具合（約5万人） | 13. ドイツ銀傘下銀行口座誤処理（復旧2日） |

# ITによる産業の高次化と社会システムの革新　～「スマートコミュニティ」～



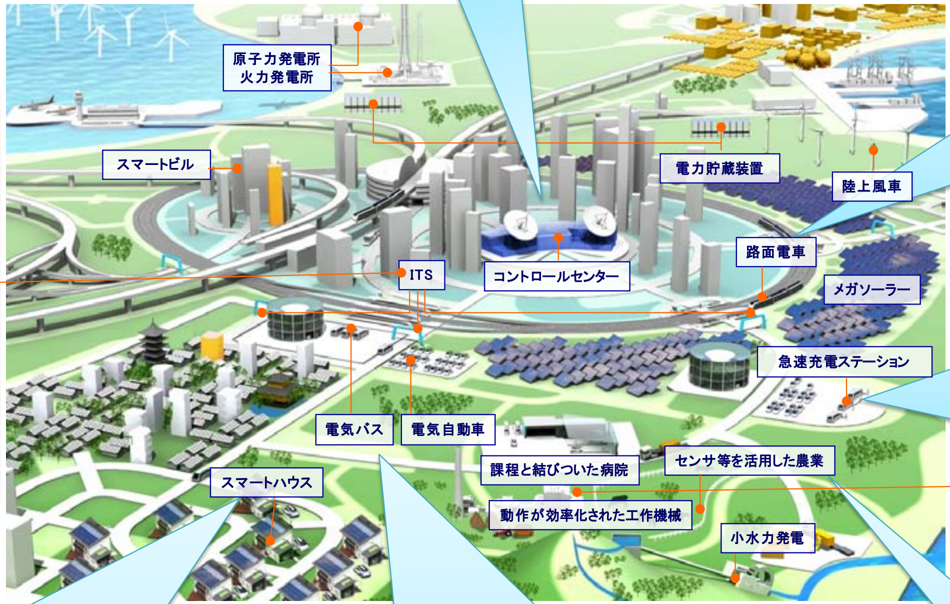
## コントロールセンター

地域のエネルギー需給を最適化するコントロールセンター

- 太陽光発電、風力発電、小水力など自然エネルギーを電源として積極的に活用
- 変動の多い自然エネルギーを地域内で有効活用するため、各家庭やオフィスで余った電力を地域内で融通
- 電気バスや電気自動車の位置情報と充電状態を管理することで、これらの自動車を電力インフラとして活用

## エネルギーネットワークと一体になった新しい交通インフラ

EVや電気バス同士で情報をやりとりすることにより、
飛躍的な低炭素化と事故や渋滞問題の解決を同時実現




## 架線レス路面電車

蓄電池を搭載した路面電車

駅での停車時：電池に充電
駅間の移動時：電池で駆動

## 急速充電ステーション

30分で80%充電

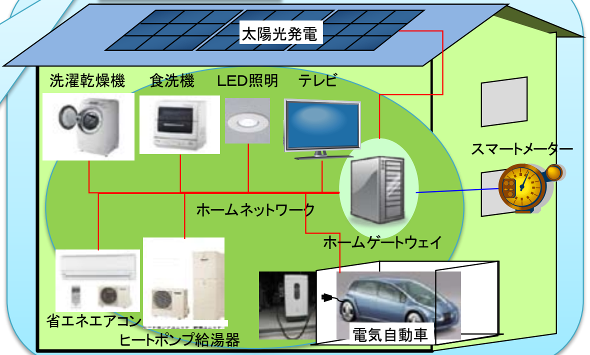
## 医療／ものづくりなど

・テーラーメード化された医療の提供
・GPSを活用した自動車両誘導システム

## EVを電力インフラとして活用

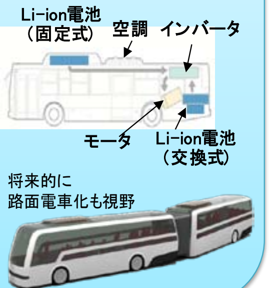
電力不足時：電気自動車→家庭
電力過剰時：家庭→電気自動車

## スマートハウス




## 電気バス（将来は路面電車化）

電池交換式の電気バス。将来的には複数台を連結して路面電車化



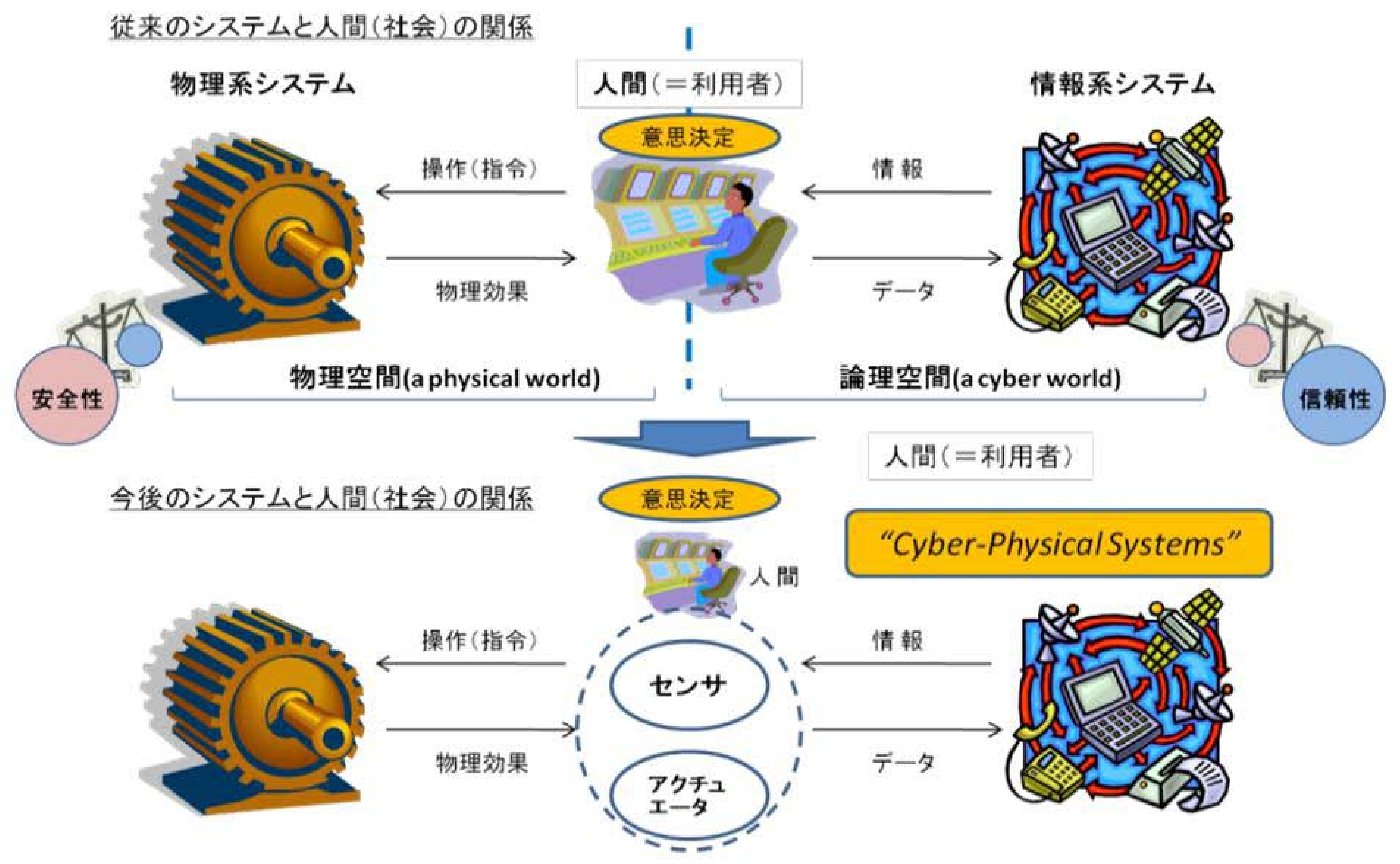

## センサ等を活用した農業

各種情報を分析し、
最適な生産手段を可能に

（出所）スマートコミュニティ関連システムフォーラム資料、三菱重工資料より経済産業省作成

# 問題を複雑にしている原因１（Cyber-Physical）

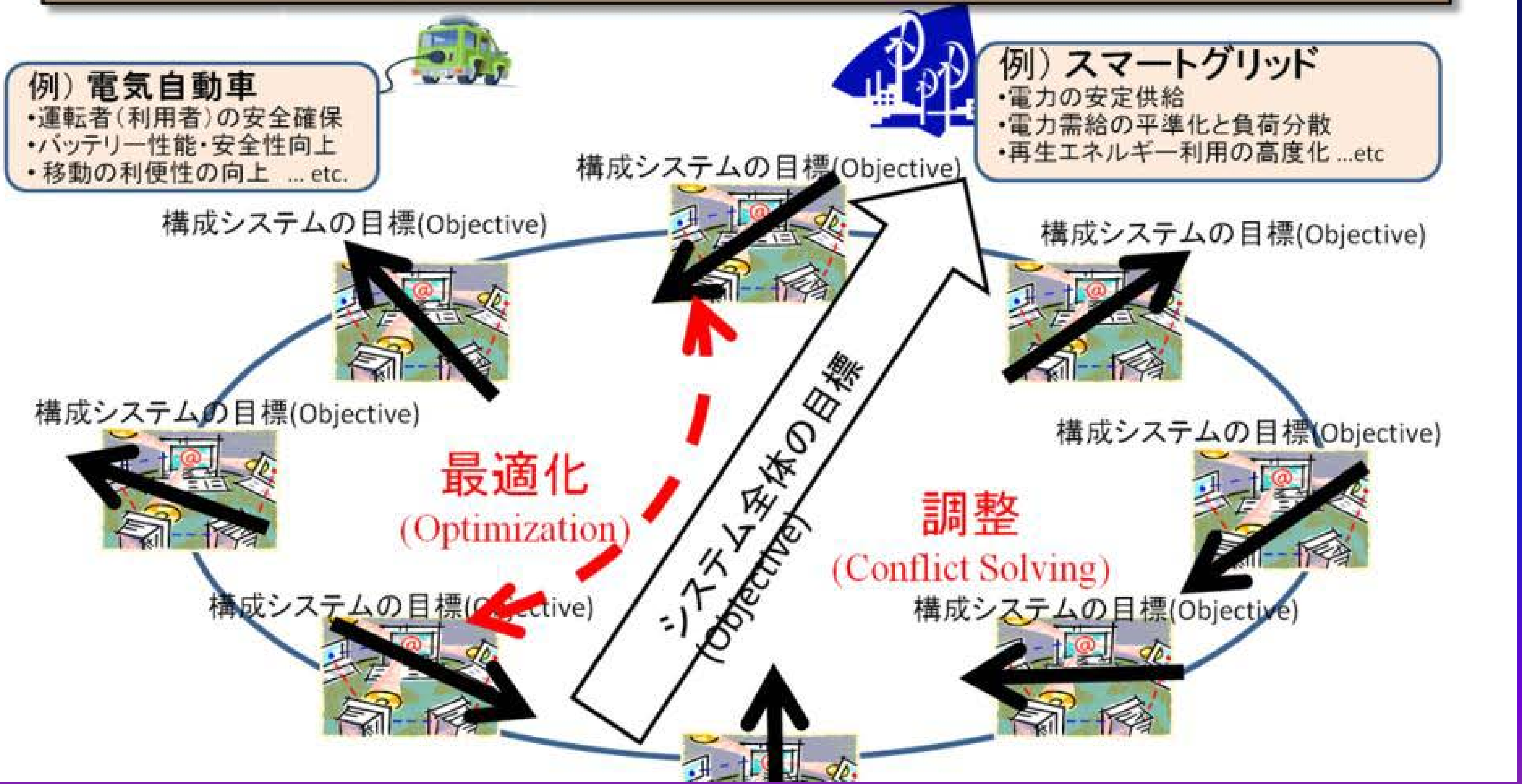




# 問題を複雑にしている原因２（System of Systems）



1. 本来の目的、ライフサイクルを異にするサブシステムから構成される複合的なシステムである。
2. 複合システムとしての全体の目的を有し、構成サブシステムはその目的に整合的に振る舞わねばならない。
3. 個々のサブシステムは各々固有の利用者（ユーザ）の要求に対し正しく機能しなければならない。
4. 個々のサブシステムの設計者には事前に全体システムの最適性を予見・評価することが出来ない。

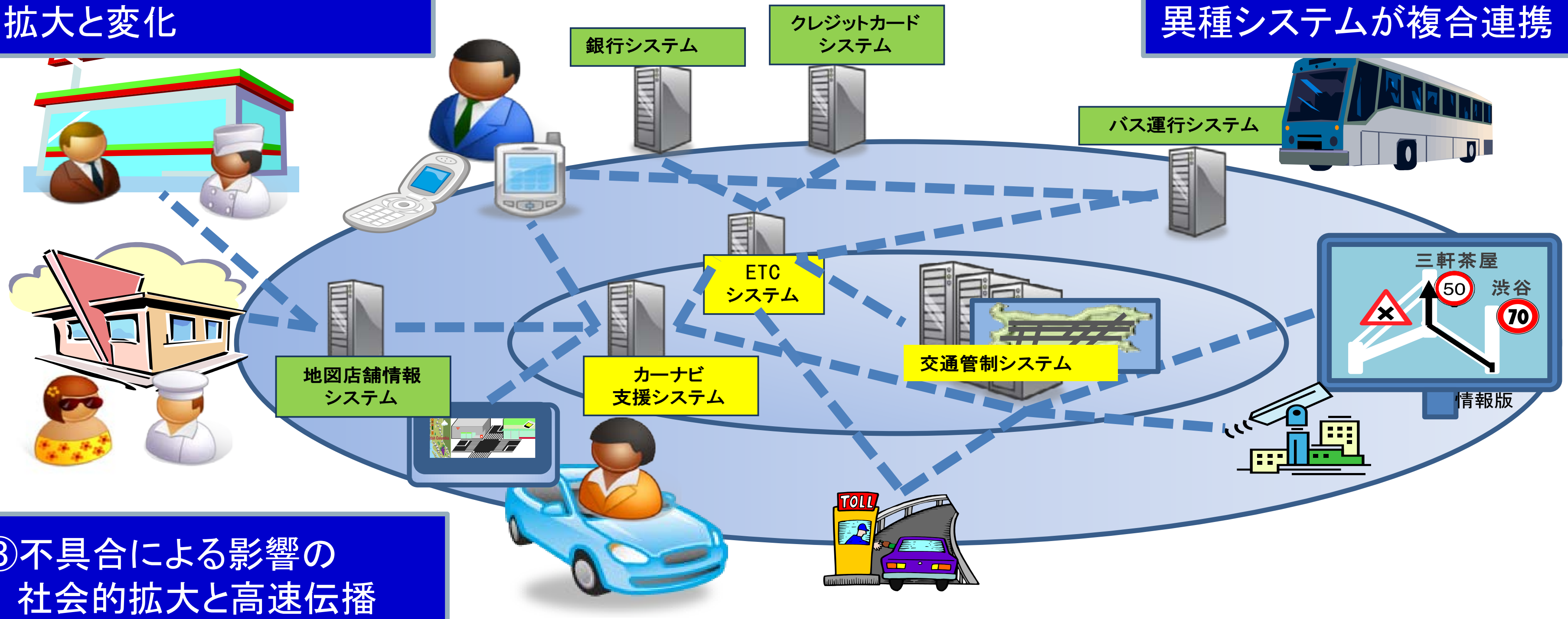


# 統合システムにおける課題

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

①利用者層・利用形態の
拡大と変化

②ライフサイクルの異なる
異種システムが複合連携




③不具合による影響の
社会的拡大と高速伝播

**ソフトウェアエンジニアリング上の課題**

①：設計段階での利用者のモデル化やシミュレーションによる利用品質の検証が不可欠。
さらに、製品投入後も利用形態の変化を継続的にモニタリングしモデル化することが必要。

②：仕様変更やシステム更改の影響予測やサービスの相互依存性など設計や運用段階でのシミュレーションが必要。

③：信頼性や安全性の客観的評価と妥当性確認に対する社会的要請に対応した検証手法や評価基準の整備が必要。

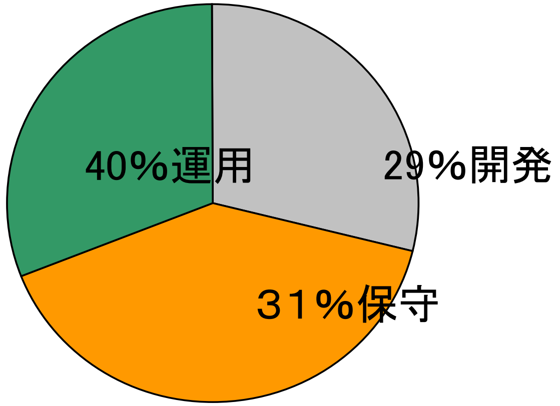
Copyright © 2009 IPA, All Rights Reserved

# 重大なシステム障害の要因分析の結果

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

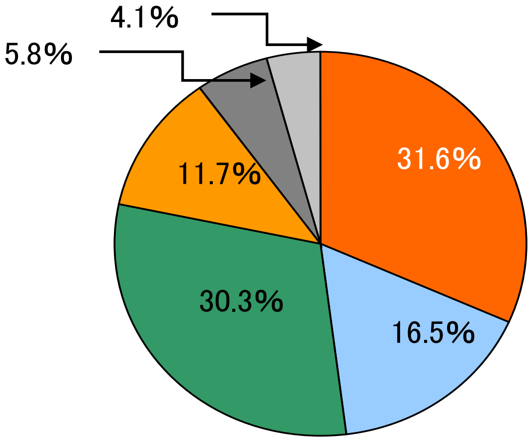
開発に起因する故障よりも、運用・保守段階に起因する故障が多い

- 85障害事例 （06年12月～08年10月）の分析例（SEC重要ｲﾝﾌﾗ研究会）




| | |
|---|---|
| 開発に係わる原因による障害 | 29% |
| 運用・保守に係わる原因による障害 | 71% |
| 運用段階での障害 | 40% |
| 保守段階での障害 | 31% |

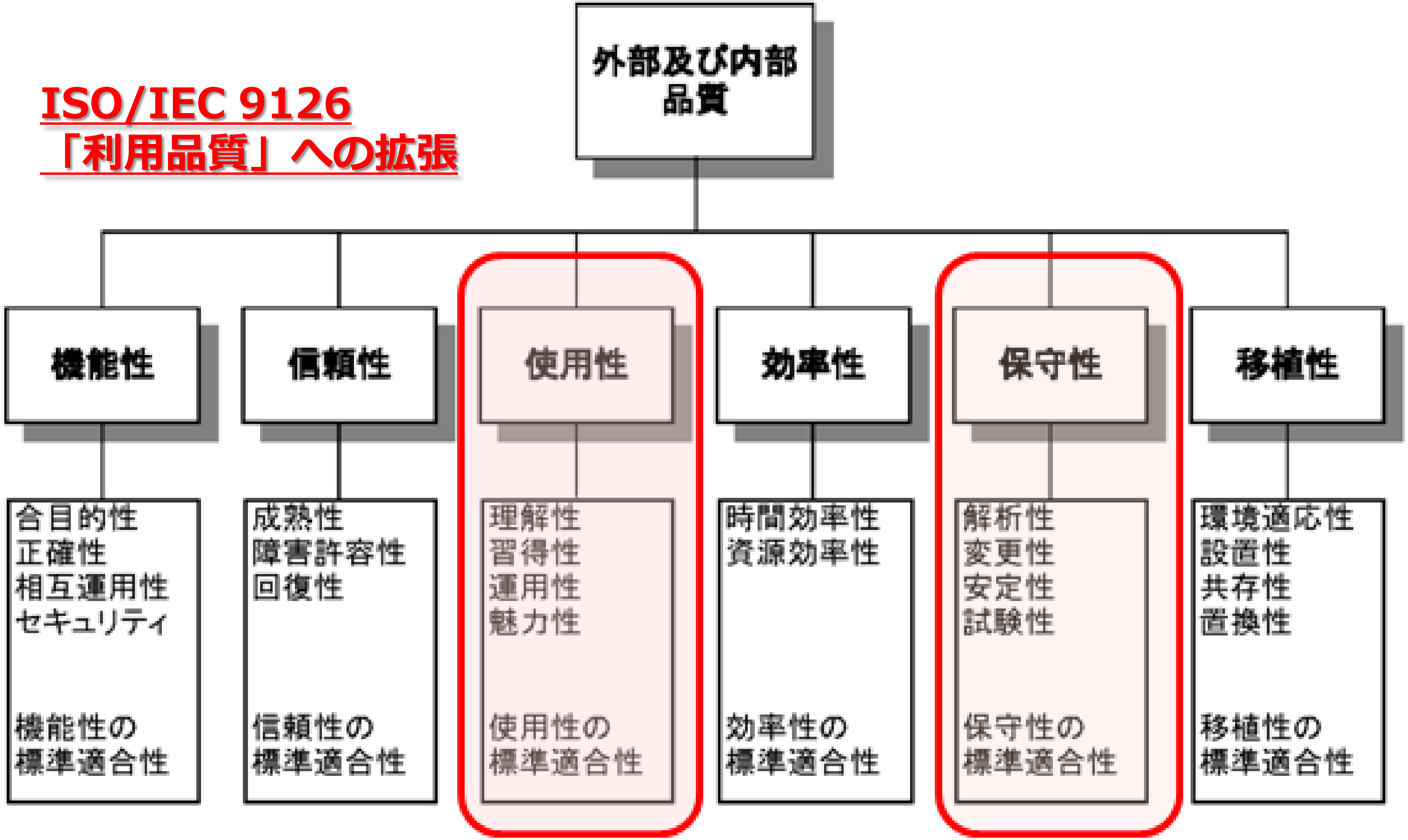
- 291障害事例（00年1月～09年8月）の分析例（日経ｺﾝﾋﾟｭｰﾀ09年8月19日号）




| | |
|---|---|
| うっかりミス | 31.6% |
| ハード故障、不慮の事故 | 16.5% |
| ソフトの不具合 | 30.3% |
| 性能・容量不足 | 11.7% |
| セキュリティ関連の不具合 | 5.8% |
| その他 | 4.1% |

# 問題を複雑にしている原因３（常に変化する利用状況）

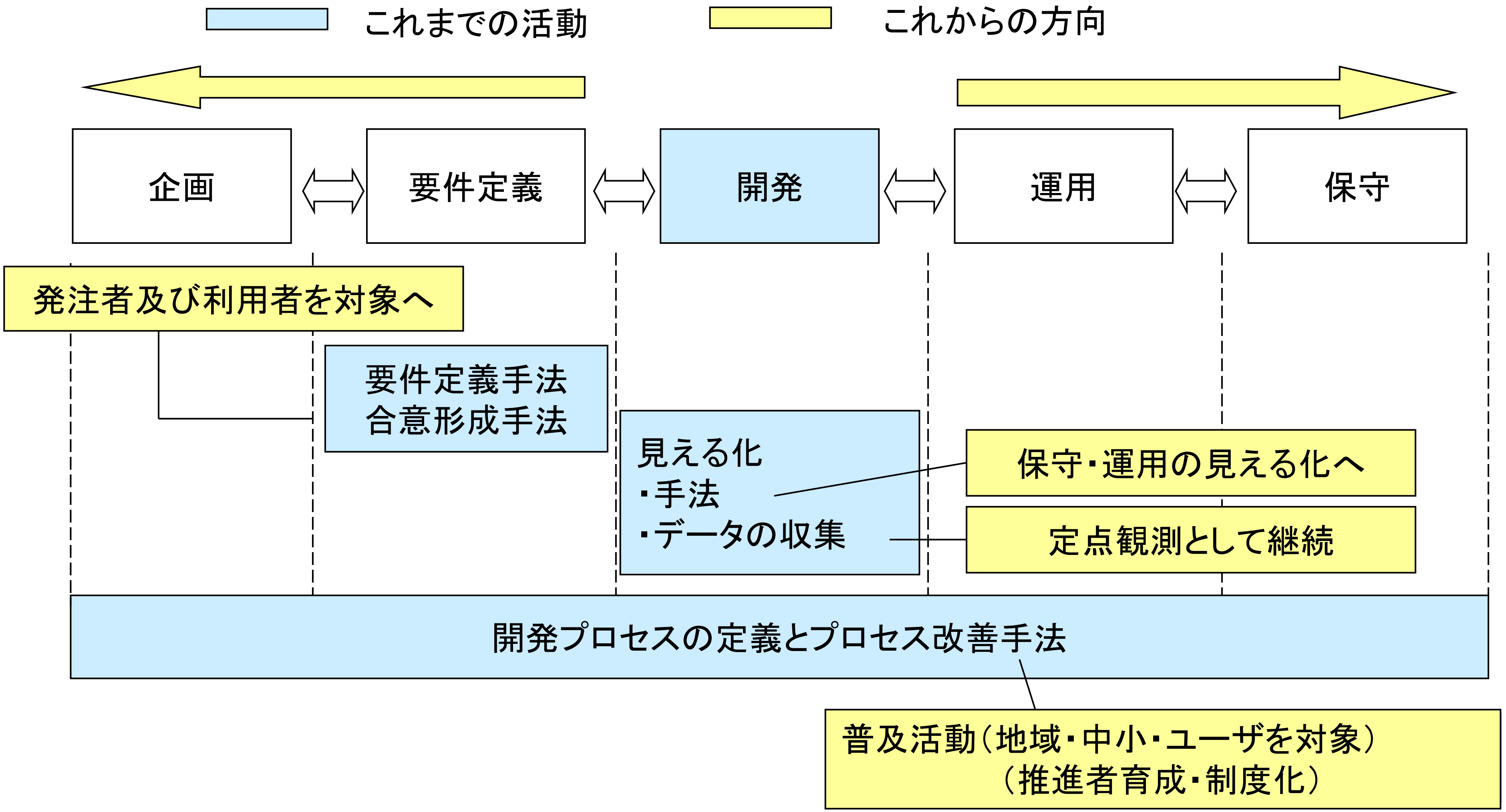





（出展） JIS X 0129:2003(ISO/IEC 9126:2001)

# 情報システムの信頼性対策の向かうべき方向

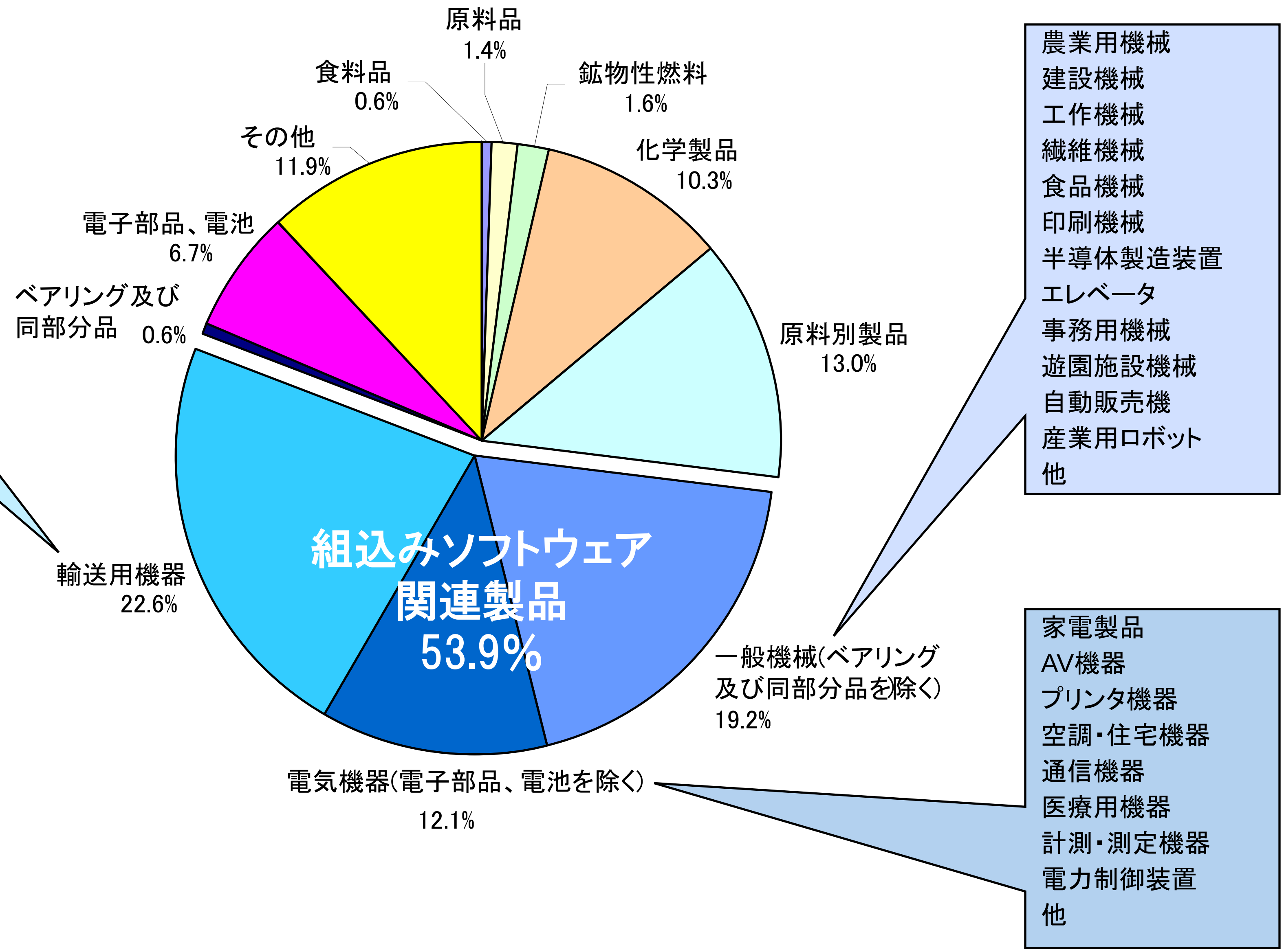


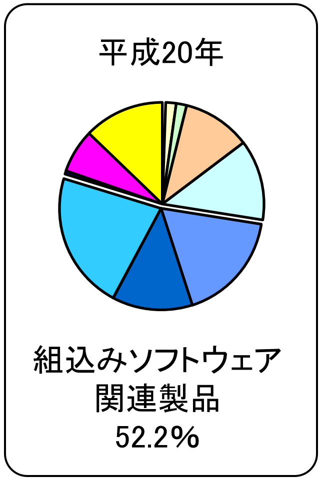


# 3. 日本の組込みソフトウェア開発現場の現状

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

## 平成21年のわが国の輸出に占める組込みソフトウェア関連製品

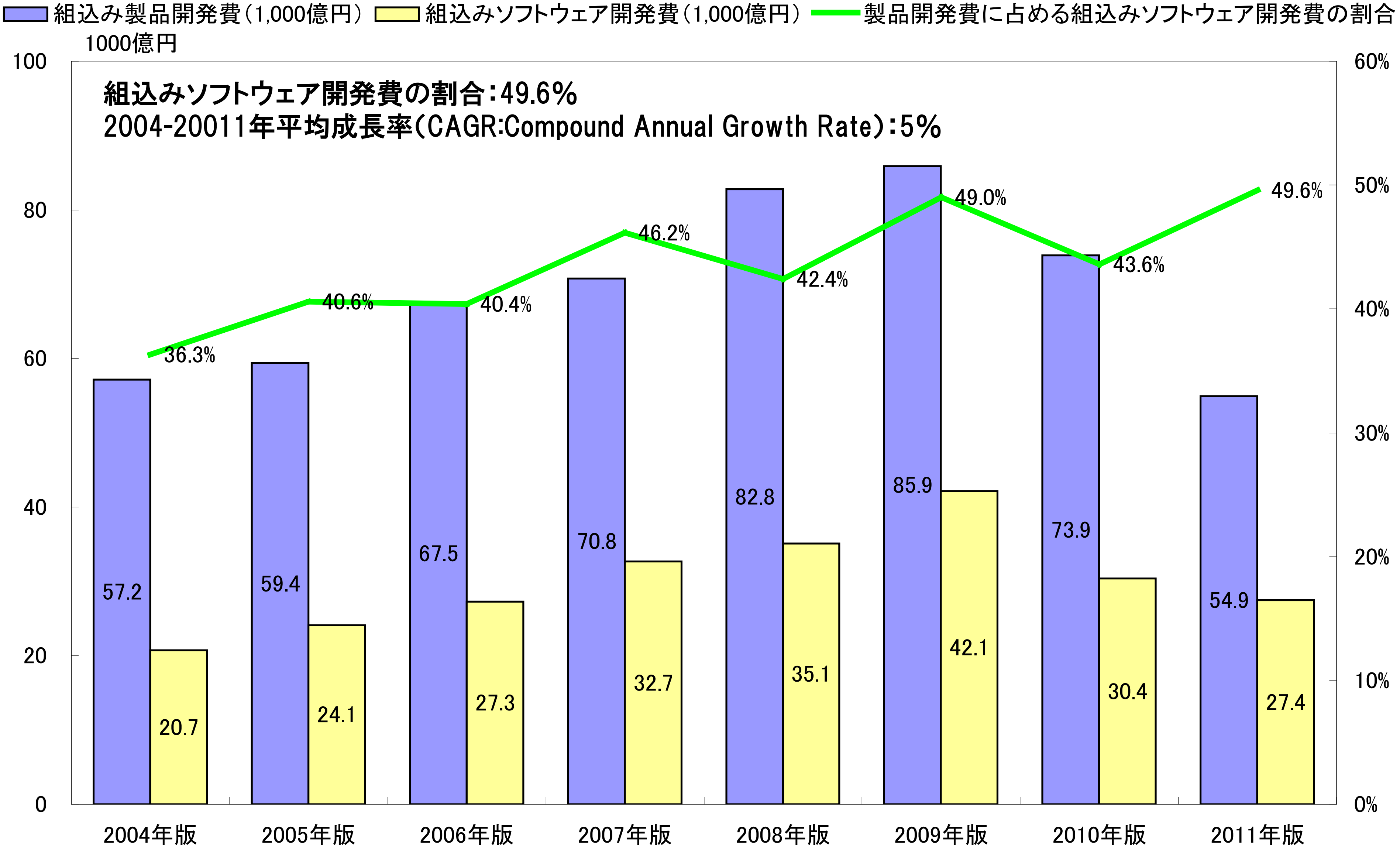



Copyright © 2011 IPA, All Rights Reserved

# 組込みシステム製品開発費と組込みソフトウェア開発費・開発費比率の推移

SEC
Software Engineering for Mo・No・Zu・Ku・Ri

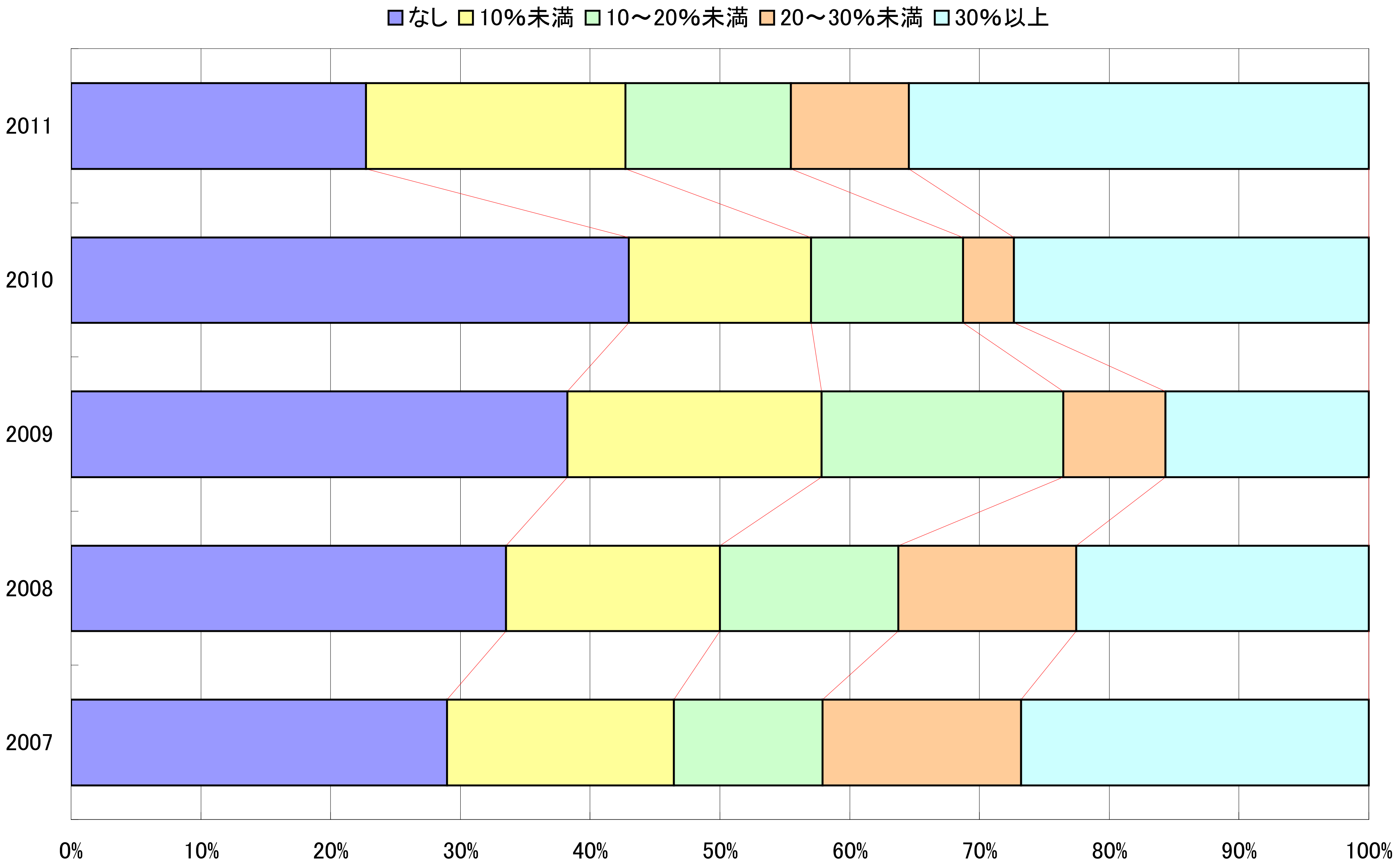



（社）日本機械工業連合会（平成21年度生産額実績統計）、組込みシステム産業の実態把握調査

Copyright © 2011 IPA, All Rights Reserved

# 製品出荷後の不具合発生製品率の推移

SEC
Software Engineering for Mo･No･Zu･Ku･Ri



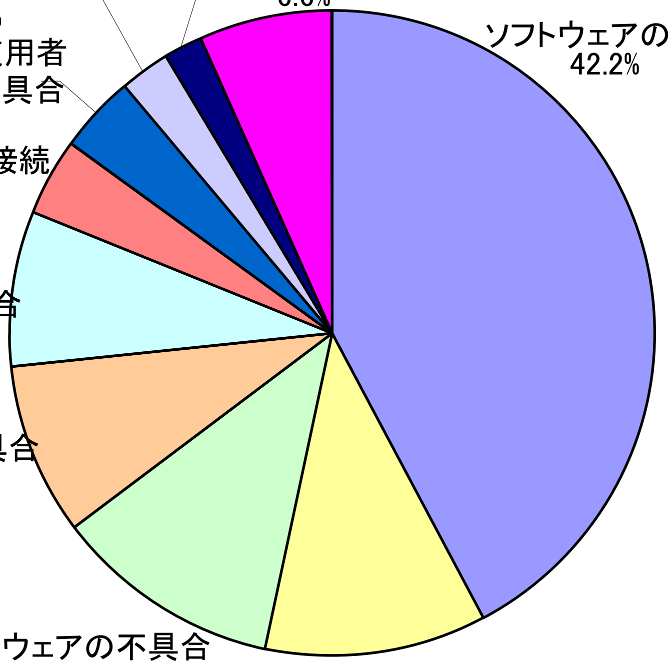

出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

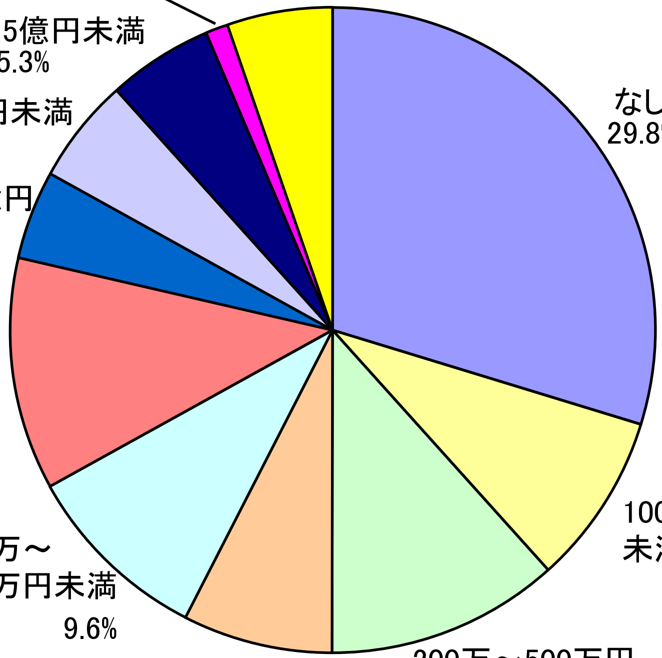
# 製品出荷後の不具合の原因と「対策費＋損失」



### 不具合の原因（製品数ベース）




### 「対策費＋損失」




出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

# 組込みソフトウェア開発課題に有効な解決手段（課題別）

SEC Software Engineering for Mo･No･Zu･Ku･Ri

| 課題＼有効な解決手段 | 技術者のスキル向上 | 開発手法・開発技術の向上 | プロジェクトマネージャのスキル向上 | 新技術の開発・導入 | 技術者の確保 | 開発環境（ツール等）の整備・改善 | 管理手法・管理技術の向上 | 委託先の確保・能力向上 | プロジェクトマネージャの確保 | 開発製品数・開発量の削減・最適化 | 経営者・投資家の理解 | 現場の理解 | 語学力の向上 | その他 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 設計品質の向上 | 68 | 44 | 31 | 15 | 27 | 19 | 27 | 10 | 14 | 10 | 6 | 5 | 2 | 1 |
| 新製品の開発 | 45 | 20 | 31 | 53 | 24 | 7 | 8 | 13 | 13 | 4 | 8 | 5 | 4 | 8 |
| 開発コストの削減 | 53 | 53 | 41 | 9 | 7 | 25 | 32 | 21 | 7 | 18 | 3 | 4 | 1 | 0 |
| 市場の拡大 | 28 | 9 | 17 | 39 | 20 | 4 | 11 | 20 | 17 | 9 | 15 | 9 | 7 | 20 |
| 開発能力（量）の向上 | 68 | 44 | 24 | 13 | 43 | 21 | 12 | 15 | 7 | 4 | 3 | 4 | 6 | 1 |
| 新技術の開発 | 66 | 30 | 14 | 70 | 38 | 5 | 0 | 9 | 7 | 5 | 7 | 4 | 4 | 2 |
| 開発期間の短縮 | 57 | 46 | 28 | 9 | 29 | 34 | 35 | 15 | 5 | 14 | 0 | 1 | 3 | 0 |
| 生産性の向上 | 73 | 55 | 32 | 11 | 9 | 43 | 25 | 9 | 5 | 5 | 2 | 7 | 0 | 2 |
| 製造品質の向上 | 73 | 36 | 32 | 36 | 32 | 0 | 32 | 14 | 18 | 23 | 9 | 14 | 0 | 5 |
| 事業環境の変化への対応 | 34 | 14 | 24 | 45 | 14 | 7 | 7 | 17 | 3 | 7 | 38 | 21 | 14 | 10 |
| 製品安全性の確保手段 | 88 | 13 | 25 | 13 | 25 | 25 | 38 | 0 | 0 | 13 | 0 | 0 | 0 | 0 |
| 規格認証等への対応手段 | 38 | 0 | 25 | 0 | 13 | 38 | 50 | 50 | 0 | 0 | 25 | 0 | 25 | 0 |
| 海外拠点・海外企業との連携手段 | 17 | 0 | 33 | 17 | 17 | 0 | 0 | 33 | 0 | 0 | 0 | 33 | 100 | 17 |
| 全体の平均 | 58 | 39 | 28 | 26 | 25 | 20 | 20 | 14 | 9 | 9 | 5 | 5 | 3 | 4 |

注：枠内の数字は課題に有効な解決手段として挙げられた1番目から3番目の合計の％

出典：「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

Copyright © 2011 IPA, All Rights Reserved

# ４．ＳＥＣにおける統合システム信頼性向上への取組み

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

**監査対象**

- ソフトウェア・プロダクト
- 開発プロセス

評価

**監査機関**
**監査人**

**監査基準**

- 基準となる品質特性
- 基準となる手法
- 基準となるプロセス など

・共通／分野別

・公平性／専門性／最新性
・国際性

・資格
・スキル／能力

**基準を支える知見**

- 高品質ソフトウェア開発・管理技術
（要件定義・上流設計・テスト
プロセス改善・定量的管理など）

品質問題の多くは要件のエラー
しかも、
人間（利用者、運用者）に絡む
↓
**上流・超上流に重点**

## 形式手法の適用

■要求定義段階での曖昧性･矛盾の排除と欠陥の早期除去

■要求～設計～実装～テストまでのトレーサビリティの確保

■形式検証によるテストの自動化

■関係者全ての間での知識共有とコミュニケーションの円滑化

# 国内の取組み事例①
# 宇宙ステーションや人工衛星における制御ソフトウェア



- **適用機関**
  - 独立行政法人 宇宙航空研究開発機構(JAXA)
- **適用目的**
  - 国際宇宙ステーションや人工衛星、地上にてそれらを運用・監視する地上システムに登載される宇宙機ソフトウェアに対し独立検証および有効性確認(IV&V: Independent Verification and Validation)を独立検証チームにより実施する。
- **形式手法の適用内容**
  - 宇宙機ソフトウェアの非機能要件（耐環境性、信頼性、可用性、資源効率性等）を満足する。耐環境性は宇宙空間という特殊な環境で継続的な動作が求められていること、信頼性は機能停止などの起きた場合に安全と経済的・社会的損失に多大な影響を及ぼすこと、可用性はいかなる状況でもミッションを達成できるようにすること、資源効率性はハードウェアリソースに厳しい制約がある中で要求された機能を満たすことである。
- **適用プロセス**
  - 要求分析、設計
- **適用技術**
  - SPIN, UPPAAL, SpecTRM(独自ツール)
- **参考文献**
  - 加藤 淳、神武 直彦、片平 真史 「宇宙機ソフトウェアに対するIV&V とその適用事例」 組込みシステムシンポジウム ESS’07 2007年10月

Copyright © 2010 IPA, All Rights Reserved

# 国内の取り組み事例②
# 携帯電話ICチップファームウェア

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- **適用機関**
  - フェリカネットワークス株式会社
- **背景**
  - 2004年7～10月にFeliCa ICチップのファームウェアの仕様を策定するための仕様策定フレームワークを開発した。これはVDM++/VDM Toolをベースとしている。その後2006年6月に最終版のROMをリリースするまで、仕様策定フレームワーク上で仕様記述を行った。
- **形式手法の適用内容**
  - 形式仕様の記述量はテストケースも含めて10万行程度である。実装コードは11万行程度になる。モバイルFeliCa ICチップは複数の半導体ベンダが製造・販売しており、それぞれでファームウェアも異なっている。しかし、異なるICチップであっても、完全な動作の互換性が求められる。そのためにも明確な仕様策定が必要であった。なお、フェリカ社で開発したモバイル FeliCa IC チップファームウェアは、Common Criteria(CC) の EAL4+ALC_FLR.1+AVA_VLA.3 の認証を受けている。
- **適用プロセス**
  - 設計
- **適用技術**
  - VDM++, VDM Tools
- **参考文献**
  - 「仕様書の記述力を鍛えるーモバイルFeliCa開発における　形式仕様記述手法の導入事例」、日経エレクトロニクス2007/02/12号 p133～152

Copyright © 2010 IPA, All Rights Reserved

# 国内の取組み事例③
# コピー複合機内の制御ソフトウェア

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- **適用機関**
  - 富士ゼロックス株式会社
- **適用目的**
  - 富士ゼロックス株式会社
- **形式手法の適用内容**
  - 検証対象のインタフェースマネージャはクラス数が60-80個であり、自動コード生成後のソースコード行数は約6万行であった。検証した状態数は1万個程度となった。適用の実際の効果に関して、テストで再現性の無い取りづらいバグの全てを取ることはできないものの、詳細設計段階において、高ストレス下で発生する可能性のある不具合を発見することができた（ストレステストの前倒し）。
  - 一方、SPINを適用する際にPromela言語仕様が課題となった。適用対象となる詳細設計仕様はC言語でかける程度の詳細な記述レベルであり、Promelaで提供している言語仕様との間に大きなギャップが存在している。
- **適用プロセス**
  - テスト
- **適用技術**
  - SPIN, Executable UML(xUML)
- **参考文献**
  - 「モデル検査でバグ発見　富士ゼロックスがMDDで－UMLから検証モデルへの変換器を開発」、日経エレクトロニクス 2006/10/23号 p34～35

Copyright © 2010 IPA, All Rights Reserved

# ソフトウェア品質監査制度(仮称)検討の背景と経緯

## 第三者の検証・妥当性確認による品質説明力強化の必要性

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

### 品質説明に対する市場意識の変化

品質説明力の不足：　当事者企業の技術的主張だけでなく、第三者の裏付け(検証、妥当性確認)による品質説明への要求の増大

### 製品の利用者が感じる違和感

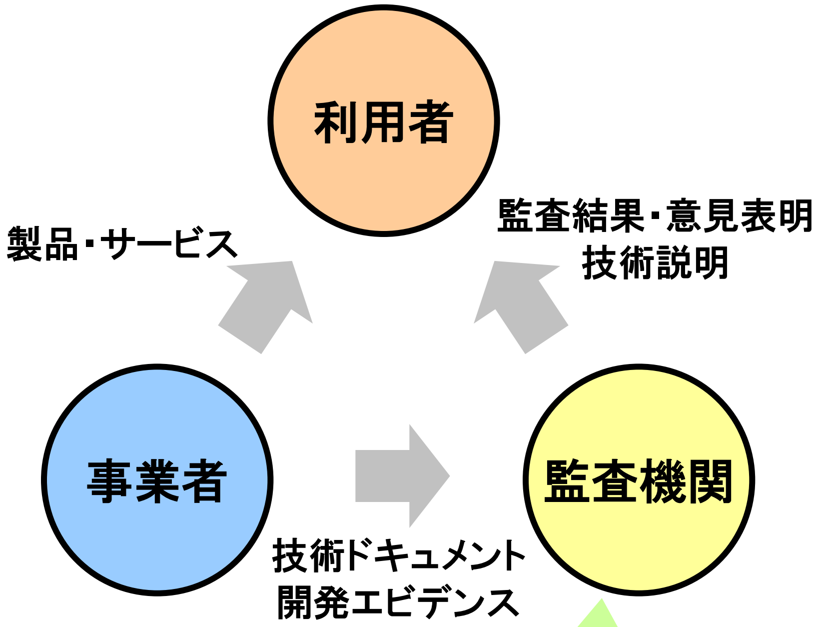
利用品質低下の懸念：　製品・システムの高度化・複雑化と利用者の多様化により、製品・システムと利用者との間のギャップが拡大

### 先端技術製品の潜在リスクへの不安

製品品質低下の懸念：　技術の急速な進歩により技術標準(規格)に基づく規格認証の対象範囲外となる領域が拡大

### 品質文化の異なる業界を跨るシステム

残存する潜在リスクの増加：　複数の業界を跨るシステムの拡大に伴い、全体システムとしての品質確認の精度が低下




### 第三者による検証・妥当性確認

事業者の技術的主張の妥当性を、監査機関が開発技術水準と利用技術水準を考慮して第三者の立場で評価し、技術に関する専門知識のない利用者にも理解できる形で情報提供する仕組み

(会計処理における会計監査と同等の役割)

### IPA/SECでの活動経緯

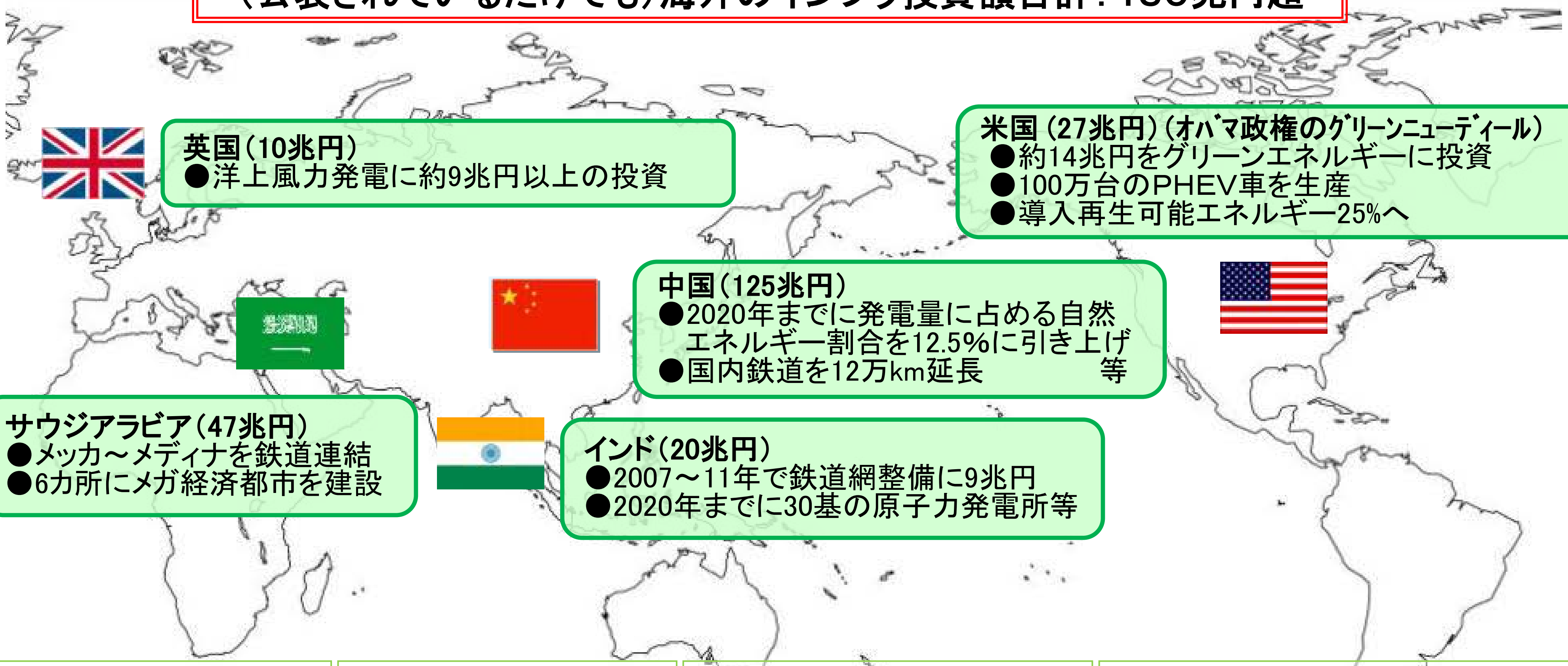
- 2010年3月：産構審情報システム・ソフトウェア小委員会にて第三者による検証・妥当性確認の枠組みの必要性が示される
- 2010年4月：IPA/SECの統合系プロジェクト内に検討チームを発足
- 2010年7月：調査活動開始
- 2010年11月：制度検討委員会発足(主査：名古屋大学高田教授)
- 2011年4月：中間報告(予定)

Copyright © 2011 IPA, All Rights Reserved

# （参考4）グリーン分野を中心とした海外の膨大なインフラ投資

➢ 先進国・新興国を問わず、グリーン分野を中心に巨額のインフラ投資を次々と計画。

**（公表されているだけでも）海外のインフラ投資額合計：430兆円超**



**英国（10兆円）**
●洋上風力発電に約9兆円以上の投資

**米国（27兆円）（オバマ政権のグリーンニューディール）**
●約14兆円をグリーンエネルギーに投資
●100万台のPHEV車を生産
●導入再生可能エネルギー25%へ

**中国（125兆円）**
●2020年までに発電量に占める自然エネルギー割合を12.5%に引き上げ
●国内鉄道を12万km延長　等

**サウジアラビア（47兆円）**
●メッカ～メディナを鉄道連結
●6カ所にメガ経済都市を建設

**インド（20兆円）**
●2007～11年で鉄道網整備に9兆円
●2020年までに30基の原子力発電所等

| **コンゴ（7.4兆円）** | **ロシア（69兆円）** | **メキシコ（29.7兆円）** | **ブラジル（32兆円）** |
|---|---|---|---|
| ●コンゴ川に世界最大の水力発電ダムを建設 | ●2030年までにシベリア鉄道を近代化 | ●5カ年の国家インフラ計画<br>●輸送・通信分野で巨額投資 | ●リオデジャネイロ～サンパウロに高速鉄道 |

その他：台湾（11兆円）、南アフリカ共和国（9兆円）、タイ（5.9兆円）、ベトナム（5.8兆円）、イラク（4.5兆円）、韓国（4兆円）、フランス（3.4兆円）など

# ソフトウェア品質監査制度(仮称)の狙いと効果
## 国民生活の安全・安心・快適の向上と我が国産業の国際競争力の強化

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

| ソフトウェア品質監査制度(仮称)の狙い | ソフトウェア品質監査制度(仮称)の効果 |
|---|---|
| 企業の製品・システムに関する利用者や市場への品質説明力の強化 | 技術の専門家ではない利用者の安心感の向上 |
| 国際市場における日本製品・システムの品質に対する正当な評価の確立 | 我が国産業の国際競争力の維持・強化 |
| 産業界の枠を超えた品質の見える化による複数の産業界を跨り構成される高度なシステムの開発加速 (例:スマートコミュニティシステムなど) | 国民生活の快適性・利便性の向上<br>新成長戦略分野における我が国産業の国際優位性の確保 |
| 製品・システムの本質的な品質向上 | 国民生活の安全性の確保 |

**ご参考:米国の状況**

- 2010年日本製自動車の制御システムに対する不具合の疑念が拡大。米国政府の要請で、NASAの独立検証・妥当性確認(IV&V)センターが第三者の立場で、制御システムの検証ならびに妥当性確認を実施。2011年2月、不具合が発見されなかったとの最終報告が公開。
- 当事者企業の主張だけでなく、第三者の主張がないと説明力が不充分との意識(会計処理における会計監査の必要性と同等の意識)。
- 国防省やNASAのシステムの調達、航空機分野、医療機器分野で類似した仕組みを運用している。

Copyright © 2011 IPA, All Rights Reserved

# 品質問題に起因する影響の度合いに応じて監査内容を定義

## 要求される品質説明力と監査コストとのバランス

SEC Software Engineering for Mo･No･Zu･Ku･Ri

利用者・国民への影響度と産業界・経済への影響度によりレベル分け(監査レベル)し、監査レベル毎に監査内容を定義する。

### 監査レベル

| 産業・経済影響レベル ＼ 利用者・国民影響レベル | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 4 | 4 | 4 | 4 | 4 | 4 |
| 3 | 3 | 3 | 3 | 3 | 4 |
| 2 | 2 | 2 | 2 | 3 | 4 |
| 1 | 1 | 1 | 2 | 3 | 4 |
| 0 | 0 | 1 | 2 | 3 | 4 |

### 監査レベルに対応した監査内容

| 監査レベル | 監査する審査項目 | 監査方法 | 独立検証 |
|---|---|---|---|
| 4 | 全項目 | 網羅監査(全件監査) | 必須 |
| 3 | 重要項目 | 網羅監査(全件監査) | 必須 |
| | その他の全項目 | 抜取監査(サンプル監査) | 任意 |
| 2 | 全項目 | 抜取監査(サンプル監査) | 任意 |
| 1 | 重要項目 | 抜取監査(サンプル監査) | 任意 |
| 0 | 非対象 | 非対象 | 非対象 |

### 産業・経済影響レベル

| レベル | 影響の範囲 |
|---|---|
| 4 | 我が国の産業への広範囲な影響 |
| 3 | 当該産業に限定された影響<br>当該企業以外の同一・類似産業のへの影響 |
| 2 | 当該企業に限定された影響<br>当該製品・サービス以外の他事業への影響 |
| 1 | 当該製品・サービス事業に限定された影響 |
| 0 | 影響はない／ほとんど影響はない |

### 利用者・国民影響レベル

| レベル | 影響の範囲・程度 |
|---|---|
| 4 | 当該利用者ならびに当該利用者以外への重大な影響(代替手段による影響軽減が困難な影響)<br>国民への広範囲で重大な影響 |
| 3 | 当該利用者への重大な影響に加え、当該利用者以外への軽微な影響(代替手段による影響軽減が容易な影響) |
| 2 | 当該利用者に限定された重大な影響 |
| 1 | 当該利用者に限定された軽微な影響 |
| 0 | 影響はない／ほとんど影響はない |

Copyright © 2011 IPA, All Rights Reserved

# ソフトウェア品質監査制度（仮称）の枠組み

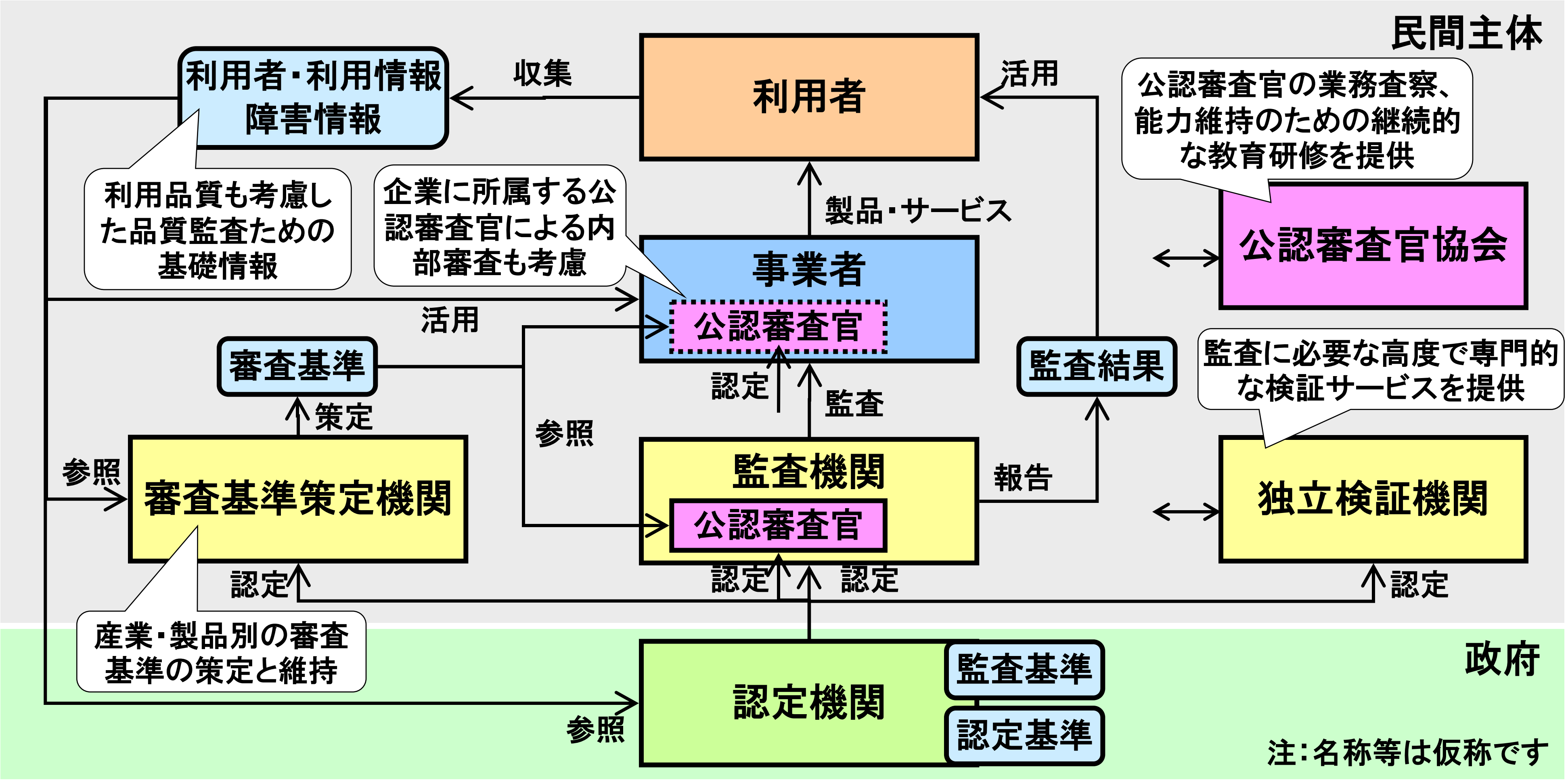
## 産業・製品分野別への対応と内部監査を考慮したフレームワーク

SEC
Software Engineering for Mo･No･Zu･Ku･Ri

下記の要件を満たす「公認審査官」が、産業分野あるいは製品分野毎に定められた「審査基準」を基に、「監査基準」に従って監査業務を遂行し、「監査結果」を利用者にも理解できる形で情報提供する制度

要件1．専門性：情報の信頼性を保証できる専門知識と能力を有していること

要件2．独立性：監査対象の事業者・利用者から身分的・経済的・精神的に独立していること




Copyright © 2011 IPA, All Rights Reserved

# 高信頼性システム開発を実現するための基準

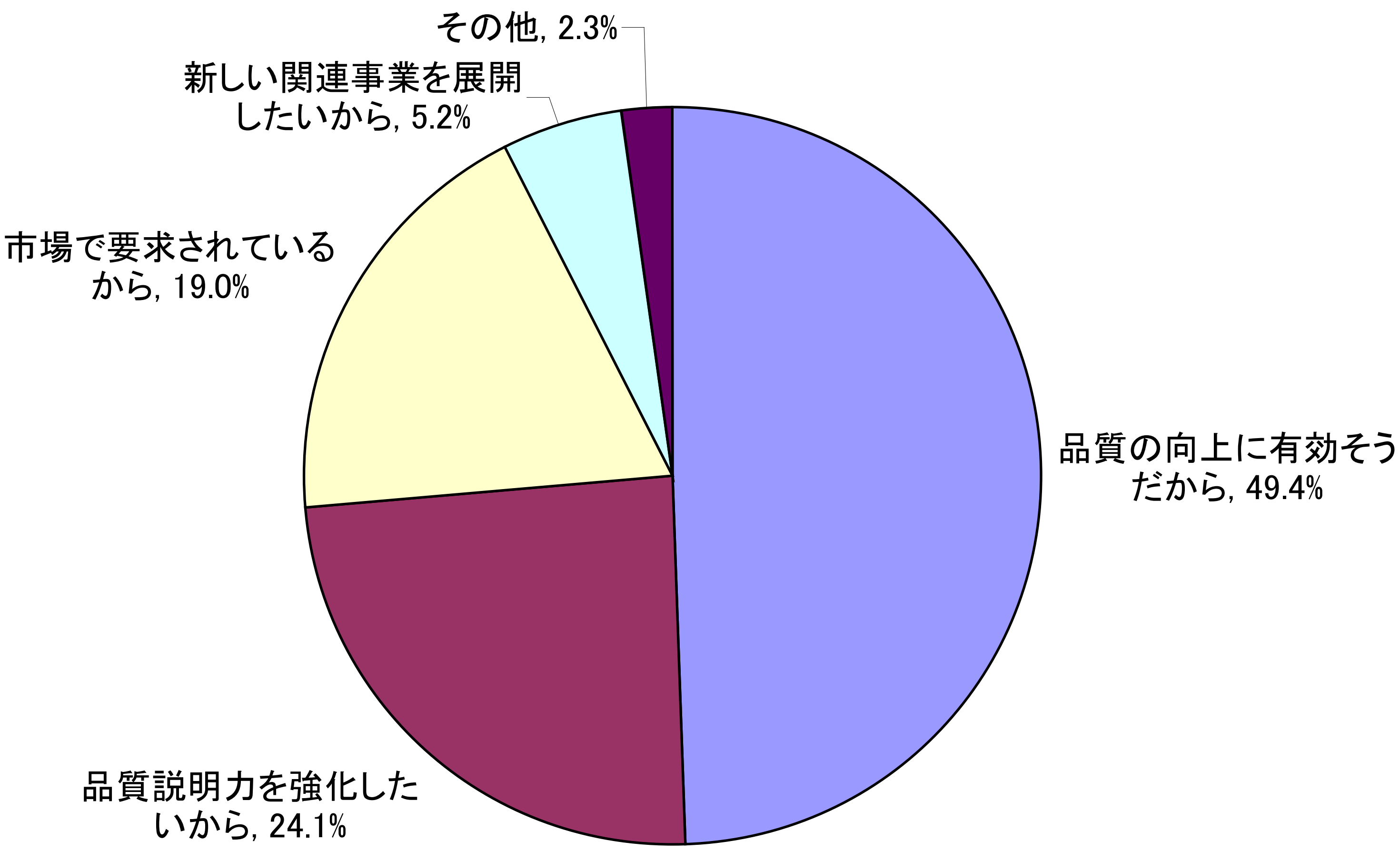


- ISO/IEC15408のEAL5～7(情報セキュリティ評価標準)
- IEC61508のSIL4(電子機器の機能安全に関する国際規格)
- ISO26262（IEC61508をベースとする自動車用組込みSWの機能安全に関する規格）
- RTCA DO-178B : Software Considerations in Airborne Systems and Equipment Certification（航空用SWの開発ガイドライン）
- Safety Related Software for Railway Signaling(鉄道信号システムおよび鉄道システムに関する規格)

Copyright © 2010 IPA, All Rights Reserved

# ESECの来場者へのアンケート結果（回答数：1985名）
# 「どのような観点で関心がありますか？」






Copyright © 2011 IPA, All Rights Reserved

# 組込みと情報処理の連携・統合



- 新たなリスクへの対応
- 異なる開発文化の擦り合わせ
- 技術・人材の共通化・流動
- 既存産業の枠組みを超えた産業連携


Copyright © 2011 IPA, All Rights Reserved